



Accounting and Information
Management Division

B-283021

June 18, 1999

The Honorable Constance A. Morella
Chairwoman
Subcommittee on Technology
Committee on Science
House of Representatives

Subject: Information Security: Subcommittee Questions Concerning the Melissa
Computer Virus

Dear Madam Chairwoman:

In response to your May 24, 1999, request, this letter provides answers to questions relating to our April 15, 1999, testimony on the immediate effects of the Melissa virus and variations of it as well as its broader implications.¹ As we noted in our testimony, although the Melissa virus did not reportedly permanently damage systems and did not compromise sensitive government data, it has shown us just how quickly computer viruses can spread and just how vulnerable federal information systems are to computer attacks. The questions and our responses follow.

1. *Since almost 2 months have passed since we first became aware of the Melissa Virus, do we now know how much damage was done and what federal agencies were affected by Melissa?*

The Melissa "Frequently Asked Questions" electronic document found at the CERT Coordination Center (http://www.cert.org/tech_tips/Melissa_FAQ.html) states that more than 300 organizations were affected, covering more than 100,000 individual hosts. These data, however, are not specific to federal agencies. As we stated in our testimony, it is critical that the federal government establish reporting mechanisms that facilitate analyses of viruses and other forms of computer attacks and their impact.

¹Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data (GAO/T-AIMD-99-146, April 15, 1999).

162347

2. *It appears from all the testimony that in terms of the actual viruses themselves, .. will always be a step behind the hackers and willful propagators of malicious code. Are there any safeguards you know of that can sniff out a virus before having seen it before, i.e., are there, or is there the possibility for, programs that can determine whether or not a program is a virus independent of being told so by a programmer?*

Antivirus tools are readily available from several commercial vendors. These tools perform three basic functions: virus detection, identification, or removal. The majority do not look for a virus unless and until the virus has been first identified and its characteristics are known. The ability to be proactive rather than reactive—that is, to defend against a virus that has never been seen before—is the basis of current antivirus research. Steve White's paper "Open Problems in Computer Virus Research" outlines research areas for antivirus tools (<http://www.av.ibm.com/InsideTheLab/Bookshelf/ScientificPapers/White/Problems/Problems.html>).

3. *You mention that unknown system vulnerabilities could lead to viral infections in the future. What are some of the things on our computers that we simply do not see as dangerous, but are instead opportunities for belligerent virus programmer. Could Java Applets and Internet cookies be used as a means of viral infections?*

Java Applets² and Internet cookies³ have many security issues associated with them. The risk is based on whether the applet actually only does what it is supposed to do, or that the system that wants to set a cookie is actually only setting a cookie. Some security analysts simply state that no user should accept either an applet or a cookie from an unknown source. However, knowing the source of the applet or cookie only means that the user knows the source, not whether the applet is malicious or that the cookie being set is the only action being taken. Also, as with all security issues, the environment is very dynamic. For example, on Princeton University's Secure Internet Computing web page, there is an announcement of a very recent Java security problem (<http://www.cs.princeton.edu/sip/History.html>). The dynamic nature of the problem means that all those involved in computing must be diligent in their security efforts.

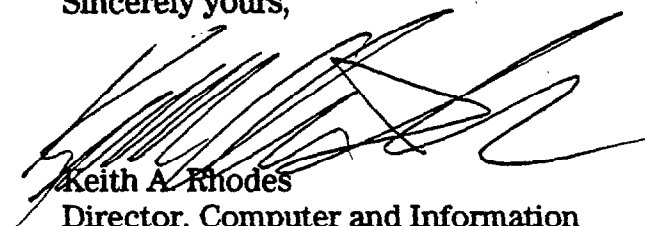
To respond to these questions, we gathered data at The Federal Computer Incident Response Capability (FedCIRC, <http://www.fedcirc.gov/>), the CERT Coordination

²A program written in the Java programming language to run within a web browser compatible with the Java platform, such as Netscape Navigator (TM).

³A "cookie" is small piece of information to help make the communication between an internet site's computer server and the browser more efficient.

Center (<http://www.cert.org>), Princeton University's office of Computing and Information Technology (CIT, <http://www.princeton.edu/cit/index.shtml>), Princeton University's Secure Internet Programming (SIP) Laboratory (<http://www.cs.princeton.edu/sip/>), the Department of Energy's Computer Incident Advisory Capability (CIAC, <http://ciac.llnl.gov/>), and the World Wide Web Consortium (W3C, <http://www.w3.org/Security/>). We conducted our work in June 1999. If you have any questions regarding this letter, please contact me at (202) 512-6415.

Sincerely yours,



Keith A. Rhodes
Director, Computer and Information
Technology Assessment

(511160)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

**U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013**

or visit:

**Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC**

**Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.**

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested